



566.40596X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: T. FUJISHIRO, et al

Serial No.: 09/941,771

Filing Date: August 30, 2001

For: CERTIFICATE VALIDITY AUTHENTICATION METHOD AND
APPARATUS

Attention: Box Missing Parts

LETTER CLAIMING RIGHT OF PRIORITY

Assistant Commissioner
for Patents
Washington, D.C. 20231

January 2, 2002

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, applicants hereby claim the right
of priority based on:

Japanese Application No. 2000-261065
Filed: August 30, 2000

A Certified Copy of said application documents are attached hereto.

Respectfully submitted,

Carl I. Brundidge
Registration No. 29,621
ANTONELLI, TERRY, STOUT & KRAUS, LLP

CIB/jdc
Enclosures
703/312-6600



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 8月30日

出 願 番 号

Application Number:

特願2000-261065

出 願 人

Applicant(s):

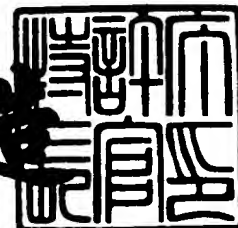
株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月31日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 HK13379000

【提出日】 平成12年 8月30日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 藤城 孝宏

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 手塚 悟

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 熊谷 洋子

【発明者】

【住所又は居所】 東京都江東区新砂一丁目6番27号 株式会社日立製作所 公共情報事業部内

【氏名】 森尾 智治

【発明者】

【住所又は居所】 東京都江東区新砂一丁目6番27号 株式会社日立製作所 公共情報事業部内

【氏名】 宮崎 豊

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100087170

【弁理士】

【氏名又は名称】 富田 和子

【電話番号】 045(316)3711

【手数料の表示】

【予納台帳番号】 012014

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】明細書

【発明の名称】証明書の有効性確認方法および装置

【特許請求の範囲】

【請求項 1】

端末からの依頼に応じて、当該端末が信頼する認証局とは異なる認証局が発行した公開鍵証明書の有効性を確認する証明書の有効性確認方法であって、

任意の認証局を起点認証局とし、当該起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先が全て端末となるまで続けることにより、前記起点認証局から任意の端末に対して公開鍵証明書を発行した端末収容認証局までのパスを検索するパス検索ステップと、

前記パス検索ステップにより検出されたパスについて、前記起点認証局を上流とし、当該パス上の端末収容認証局が発行した公開鍵証明書の署名を 1 つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は当該 1 つ上流側の認証局が発行した公開鍵証明書の署名をさらに 1 つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該 1 つ上流側の認証局が前記起点認証局となるまで続けることにより、当該パスを検証するパス検証ステップと、

前記パス検証ステップにより検証が成立したパスをデータベースに登録するパス登録ステップと、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されているときに、前記公開鍵証明書の有効性が確認されたものと判断する有効性確認ステップと、を有すること

を特徴とする証明書の有効性確認方法。

【請求項 2】

請求項 1 記載の証明書の有効性確認方法であって、

前記パス検索ステップは、定期的に実行され、

前記パス検証ステップは、前記パス検索ステップにより検索された最新のパス

に対して実行され、そして、

前記パス登録ステップは、前記データベースの登録内容を、前記パス検証ステップで検証が成立した最新のパスに更新すること

を特徴とする証明書の有効性確認方法。

【請求項3】

請求項1または2記載の証明書の有効性確認方法であって、

前記パス登録ステップにより前記データベースに登録されている各パスについて、当該パス上の各認証局が発行した1つ下流側の認証局（発行元が端末収容認証局の場合は、当該認証局が収容する端末）に対する公開鍵証明書各々の有効期限を調べる有効期限調査ステップと、

前記有効期限調査ステップにより有効期限を過ぎていることが確認された公開鍵証明書の発行元から、当該公開鍵証明書の発行先に対する新たな公開鍵証明書を入手し、少なくとも、当該新たな公開鍵証明書の署名を、前記発行元より1つ上流側の認証局が発行した公開鍵証明書で検証するパス再検証ステップと、をさらに有し、

前記パス登録ステップは、

前記パス再検証ステップにて前記新たな公開鍵証明書の署名検証が成立しなかった場合、あるいは、前記新たな公開鍵証明書を入手できなかった場合は、前記有効期限調査ステップにより有効期限を過ぎていることが確認された公開鍵証明書の発行元と発行先とを含むパスを、前記データベースから削除すること

を特徴とする証明書の有効性確認方法。

【請求項4】

請求項1、2または3記載の証明書の有効性確認方法であって、

前記パス登録ステップにより前記データベースに登録されている各パスについて、当該パス上の各認証局が発行した公開鍵証明書の失効情報を調査する失効情報調査ステップをさらに有し、

前記パス登録ステップは、

前記失効情報調査ステップにより失効していることが確認された公開鍵証明書の発行元と発行先とを含むパスが前記データベースに登録されている場合は、こ

れを前記データベースから削除すること

を特徴とする証明書の有効性確認方法。

【請求項 5】

請求項 1、2、3 または 4 記載の証明書の有効性確認方法であって、

前記有効性確認ステップは、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されている場合でも、この 2 つのパス上のいずれかの認証局が発行した、当該認証局が位置するパス上の 1 つ下流側の認証局（発行元が端末収容認証局の場合は、当該認証局が収容する端末）に対する公開鍵証明書中に、前記 2 つのパス上のいずれかの認証局を信頼しない旨の制限が記述されている場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること

を特徴とする証明書の有効性確認方法。

【請求項 6】

請求項 1、2、3、4 または 5 記載の証明書の有効性確認方法であって、

前記有効性確認ステップは、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されている場合でも、この 2 つのパス上のいずれかの認証局が発行した、当該認証局が位置するパス上の 1 つ下流側の認証局（発行元が端末収容認証局の場合は、当該認証局が収容する端末）に対する公開鍵証明書中に記述されているパス長（パス上の許容最大認証局数）を、前記 2 つのパス上の認証局の合計数が超えている場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること

を特徴とする証明書の有効性確認方法。

【請求項 7】

請求項 1、2、3、4、5 または 6 記載の証明書の有効性確認方法であって、
前記有効性確認ステップは、

端末から、当該端末が行おうとしている電子手続に要求される信頼度の提示を伴った、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されている場合でも、この 2 つのパス上のいずれかの認証局が発行した、当該認証局が位置するパス上の 1 つ下流側の認証局（発行元が端末収容認証局の場合は、当該認証局が収容する端末）に対する公開鍵証明書中に記述されている信頼度（ポリシー）が、前記電子手続に要求される信頼度よりも低い場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること

を特徴とする証明書の有効性確認方法。

【請求項 8】

請求項 1、2、3、4、5、6 または 7 記載の証明書の有効性確認方法であって、

前記起点認証局は、

少なくとも 2 つのセキュリティドメインのルート認証局各々と相互認証を行っているブリッジ認証局であること

を特徴とする証明書の有効性確認方法。

【請求項 9】

端末からの依頼に応じて、当該端末が信頼する認証局とは異なる認証局が発行した公開鍵証明書の有効性を確認する証明書の有効性確認装置であって、

任意の認証局を起点認証局とし、当該起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先が全て端末となるまで続けることにより、前記起点認証局から任意の端末に対して公開鍵証明書を発行した端末収容認証局までのパスを検索するパス検索手段と、

前記パス検索手段により検出されたパスについて、前記起点認証局を上流とし

、当該パス上の端末収容認証局が発行した公開鍵証明書^の署名を1つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は当該1つ上流側の認証局が発行した公開鍵証明書の署名をさらに1つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該1つ上流側の認証局が前記起点認証局となるまで続けることにより、当該パスを検証するパス検証手段と、

前記パス検証手段により検証が成立したパスをデータベースに登録するパス登録手段と、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されているときに、前記公開鍵証明書の有効性が確認されたものと判断する有効性確認手段と、を有すること

を特徴とする証明書の有効性確認装置。

【請求項10】

端末からの依頼に応じて、当該端末が信頼する認証局とは異なる認証局が発行した公開鍵証明書の有効性を確認するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読み取られて実行されることで、

任意の認証局を起点認証局とし、当該起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先が全て端末となるまで続けることにより、前記起点認証局から任意の端末に対して公開鍵証明書を発行した端末収容認証局までのパスを検索するパス検索手段と、

前記パス検索手段により検出されたパスについて、前記起点認証局を上流とし、当該パス上の端末収容認証局が発行した公開鍵証明書の署名を1つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は当該1つ上流側の認証局が発行した公開鍵証明書の署名をさらに1つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該1つ上流側の認証局が前記起点認証局となるまで続けることにより、当該パスを検証するパス検証手段と、

前記パス検証手段により検証が成立したパスをデータベースに登録するパス登録手段と、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されているときに、前記公開鍵証明書の有効性が確認されたものと判断する有効性確認手段とを、当該電子計算機上に構築すること

を特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、PKI (Public Key Infrastructure) において、ある端末が受け取った電子手続に対する署名を検証するための公開鍵証明書が、当該端末が信頼する認証局とは異なる認証局が発行したものである場合に、その有効性を確認するのに好適な技術に関する。

【0002】

【従来の技術】

民間系、公共系の様々な組織、団体において、従来、紙面で行ってきた様々な手続を電子化するべく、PKI (Public Key Infrastructure) の導入、整備が進んでいる。

【0003】

図12は、従来のPKIにおいて、認証局が複数ある場合における各認証局の関係を示している。

【0004】

図示するように、公開鍵証明書の発行とその管理を行う各認証局は、ルート認証局CA1を頂点とするツリー構造を持つグループを形成している。このグループはセキュリティドメインと呼ばれている。ルート認証局CA1は、自身より1つ下流側に位置する各認証局CA2₁~CA2_nに対して公開鍵証明書を発行する

。また、認証局 $CA2_1 \sim CA2_{n1}$ 各々は、自身より1つ下流側に位置する各認証局 $CA3_1 \sim CA3_{n2}$ に対して公開鍵証明書を発行する。このように、ツリー上、1つ上流側に位置する認証局が自身より1つ下流側に位置する認証局に対して公開鍵証明書を発行する。そして、ツリー上、最下流に位置する認証局（以下、端末収容認証局と呼ぶ） $CAS_1 \sim CAS_{nm}$ は、電子手続を行うユーザ端末（以下、エンドエンティティと呼ぶ） $EE_1 \sim EE_x$ に対して公開鍵証明書を発行する。

【0005】

エンドエンティティ $EE_1 \sim EE_x$ 各々が電子文書の署名に使用する秘密鍵（署名鍵）の正当性は、自身を収容する端末収容認証局 $CAS_1 \sim CAS_{nm}$ が発行した公開鍵証明書によって証明され、端末収容認証局 $CAS_1 \sim CAS_{nm}$ 各々が発行する公開鍵証明書の署名に使用する秘密鍵の正当性は、自身を収容する認証局 $CA(S-1)_1 \sim CA(S-1)_{n(m-1)}$ が発行した公開鍵証明書によって証明される。したがって、エンドエンティティ $EE_1 \sim EE_x$ 各々が署名に使用する秘密鍵は、最終的に、ルート認証局 $CA1$ が発行する公開鍵証明書によって証明されることになる。このエンドエンティティ $EE_1 \sim EE_x$ が署名に使用する鍵の正当性を最終的に証明する認証局、云いかえれば、エンドエンティティ $EE_1 \sim EE_x$ が信頼する、ツリー上、最上流側の認証局をトラストアンカーと呼ぶ。

【0006】

さて、図12において、エンドエンティティ EE_1 は、エンドエンティティ EE_x に送信すべき申請書等の電子文書に対して、エンドエンティティ EE_1 が保持する自身の秘密鍵で署名を行う。そして、署名した電子文書に、エンドエンティティ EE_1 を収容する端末収容認証局 CAS_1 が発行した前記秘密鍵と対の公開鍵証明書を添付して、エンドエンティティ EE_x に送信する。

【0007】

エンドエンティティ EE_x は、エンドエンティティ EE_1 より受け取った電子文書の署名を、当該電子文書に添付された公開鍵証明書を用いて検証することができる。しかし、公開鍵証明書はエンドエンティティ EE_x を収容する端末収容認証局 CAS_{nm} が発行したものではないので、エンドエンティティ EE_x は、当該

公開鍵証明書を直ちに信頼することはできない。この場合、エンドエンティティ EE_x は、自身のトラストアンカーであるルート認証局 CA_1 によって当該公開鍵証明書の有効性が証明されるものであることを確認しなければならない。この公開鍵証明書の有効性確認処理は、以下の手順によって行われる。

【0008】

①トラストアンカーから公開鍵証明書の発行元認証局までのパスの検索

トラストアンカー（ここでは、ルート認証局 CA_1 ）を起点認証局とし、起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先に、公開鍵証明書の発行元認証局（ここでは、エンドエンティティ EE_1 を収容する端末収容認証局 CAS_1 ）が含まれるまで続け、トラストアンカーから公開鍵証明書の発行元認証局までのパスを検索する。

【0009】

②検出したパスの検証

上記①により検出したパス上の各認証局から、パス上において当該認証局の1つ下流側の認証局に対して発行した公開鍵証明書を入手する。そして、有効性確認対象の公開鍵証明書（ここでは、端末収容認証局 CAS_1 がエンドエンティティ EE_1 に対して発行した公開鍵証明書）の署名を、当該公開鍵証明書を発行した認証局（ここでは、端末収容認証局 CAS_1 ）より1つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は、当該1つ上流側の認証局が発行した公開鍵証明書の署名をさらに1つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該1つ上流側の認証局がトラストアンカーとなるまで続ける。そして、このような公開鍵証明書の署名検証がトラストアンカーまで成立した場合に、有効性確認対象の公開鍵証明書の有効性が確認されたものとする。

【0010】

エンドエンティティ EE_x は、エンドエンティティ EE_1 より受け取った電子文書の署名を当該電子文書に添付された公開鍵証明書をを用いて検証すると共に、上記の①、②に示す手順に従い当該電子文書の署名検証に用いた公開鍵証明書の有効性を確認することにより、当該電子文書の正当性を確認することができる。

【 0 0 1 1 】

なお、以上では、公開鍵証明書の有効性確認処理をエンドエンティティで行うことを前提としている。しかし、公開鍵証明書の有効性確認処理は負荷が重く、これをエンドエンティティで行うためには、当該エンドエンティティに高い処理能力が要求される。そこで、ネットワークを介してエンドエンティティに接続された証明書の有効性確認サーバを設け、当該サーバに、当該エンドエンティティの代わりに公開鍵証明書の有効性確認を行わせることが I E T F により提案されている。

【 0 0 1 2 】

【発明が解決しようとする課題】

ところで、従来提案されている証明書の有効性確認サーバは、エンドエンティティから依頼を受ける都度、上記の①、②に示す手順を実行して公開鍵証明書の有効性を確認している。このため、エンドエンティティが公開鍵証明書の有効性確認を依頼をしてからその結果がわかるまでに、少なくとも、上記の①、②に示す手順を実行するための時間がかかってしまう。

【 0 0 1 3 】

なお、図 1 2 では、セキュリティドメインが 1 つであることを前提にしているが、上述したように、民間系、公共系の様々な組織、団体において P K I の導入、整備が行われており、その結果、複数のセキュリティドメインが並存することが予想される。これらの異なるセキュリティドメイン間においても、各セキュリティドメインのルート認証局同士で、互いに相手の公開鍵証明書を発行するなどして相互認証を行ったり、あるいは、各セキュリティドメインのルート認証局各々との間でこのような相互認証を行ったブリッジ認証局を設置することにより、上記の①、②にその手順を示した公開鍵証明書の有効性確認処理を実現することができる。しかしこのように、複数のセキュリティドメイン間で公開鍵証明書の有効性確認処理を行うと、認証局数が増大し、また、各認証局の関係も、図 1 2 に示すような単純なツリー構造ではなく、より複雑化するため、上記の①、②に示す手順を実行するための負荷が増大する。このため、エンドエンティティが公開鍵証明書の有効性確認を依頼をしてからその結果がわかるまでにかかる時間が

さらに長くなり、サービスの低下を招いてしまう。

【0014】

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短くすることにある。

【0015】

【課題を解決するための手段】

上記課題を解決するために、本発明では、ネットワークを介して、複数の端末（エンドエンティティ）や認証局に接続された証明書の有効性確認サーバにおいて、ある端末からの依頼に応じて、当該端末が信頼する認証局とは異なる認証局が発行した公開鍵証明書の有効性を確認するために以下の処理を行う。

【0016】

すなわち、任意の認証局を起点認証局とし、当該起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先が全て端末となるまで続けることにより、前記起点認証局から任意の端末に対して公開鍵証明書を発行した端末収容認証局までのパスを検索するパス検索ステップと、

前記パス検索ステップにより検出されたパスについて、前記起点認証局を上流とし、当該パス上の端末収容認証局が発行した公開鍵証明書の署名を1つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は当該1つ上流側の認証局が発行した公開鍵証明書の署名をさらに1つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該1つ上流側の認証局が前記起点認証局となるまで続けることにより、当該パスを検証するパス検証ステップと、

前記パス検証ステップにより検証が成立したパスをデータベースに登録するパス登録ステップとを、端末からの公開鍵証明書の有効性確認依頼とは無関係に、例えば定期的に行う。

【0017】

そして、ある端末から、当該端末が信頼する認証局とは異なる端末収容認証局

が発行した公開鍵証明書の有効性確認依頼があった場合に、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されているか否かを調べることで、前記公開鍵証明書の有効性を確認する。

【0018】

本発明によれば、ある端末から公開鍵証明書の有効性確認依頼を受けた場合に、それから、上記の①、②に示した、当該端末のトラストアンカーから当該公開鍵証明書の発行元認証局までのパスの検索、および、検出したパスの検証を行う必要がない。したがって、公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短縮できる。

【0019】

【発明の実施の形態】

以下に、本発明の一実施形態について説明する。

【0020】

図1は、本発明の一実施形態が適用されたPKIシステムの概略構成を示す図である。

【0021】

図示するように、本実施形態のPKIシステムは、電子手続を行うユーザ端末あるいはユーザ端末からの依頼を受けて電子手続を代行する受付サーバである複数のエンドエンティティEEと、公開鍵証明書の発行とその管理を行う複数の認証局CAと、エンドエンティティEEからの依頼に応じ公開鍵証明書の有効性の確認を行う証明書有効性確認センタVCとが、LAN、WANおよびこれらを繋ぐインターネット等により構成されたネットワークNETを介して、互いに接続されて構成される。

【0022】

図2は、図1に示すPKIシステムでの各認証局CAの関係の一例を示す図である。

【0023】

図示するように、本実施形態のPKIシステムでは、民間系、政府系といった

複数のセキュリティドメインSD ($SD_1 \sim SD_3$) が並存していることを前提としている。そして、そのうちの幾つかのセキュリティドメインSD (図2では SD_2 、 SD_3) は、ルート認証局CA (図2では CA_{21} 、 CA_{31}) 同士で、例えば互いに公開鍵証明書を発行し合うことにより相互認証を行っているものとする。また、各セキュリティドメインSDのルート認証局CA (図2では CA_{11} 、 CA_{21} 、 CA_{31}) は、例えば、ブリッジ認証局 CA_{bridge} に対して公開鍵証明書を発行すると共に、ブリッジ認証局 CA_{bridge} から公開鍵証明書を発行してもらうことにより、ブリッジ認証局 CA_{bridge} との間で相互認証を行っているものとする。このようにすることで、あるセキュリティドメインSDに属する認証局CAと他のセキュリティドメインSDに属する認証局CAとの間に、一方の認証局CAが発行した公開鍵証明書の有効性を、他方の認証局CAにて確認できるようにするためのパスが形成される。

【0024】

次に、上記のPKIシステムを構成するエンドエンティティEE、認証局CAおよび証明書有効性確認センタVCについて説明する。

【0025】

まず、エンドエンティティEEについて説明する。

【0026】

図3は、エンドエンティティEEの概略構成を示す図である。

【0027】

図示するように、エンドエンティティEEは、処理部10aと、記憶部10bと、ネットワークNETを介して他装置と通信を行うための通信部16と、ユーザが作成した電子文書や他のエンドエンティティEEあるいはユーザ端末から受け取った電子文書の入出力やユーザよりの指示の受付けを行う入出力部17と、を有する。

【0028】

処理部10aは、署名生成部14と、署名検証部15と、エンドエンティティEEの各部を統括的に制御する制御部18と、を有する。

【0029】

記憶部10bは、ユーザが作成した（エンドエンティティEEが受付サーバの場合はユーザ端末から受け取った）電子文書を保持する電子文書保持部11と、秘密鍵（署名鍵）とこれに対する公開鍵証明書とを保持する鍵保持部12と、他のエンドエンティティEEから受け取った署名付きの電子文書と公開鍵証明書を保持する検証対象保持部13と、を有する。

【0030】

このような構成において、制御部18は、入出力部17を介してユーザから、電子文書保持部11に保持してある電子文書を他のエンドエンティティEEに送信すべき旨の指示を受け付けると、当該電子文書を電子文書保持部11から読み出し、これを署名生成部14に渡す。これを受けて、署名生成部14は、鍵保持部12に保持されている秘密鍵を用いて当該電子文書に対する署名を生成する。それから、制御部18は、電子文書保持部11から読み出した電子文書に署名生成部14で生成された署名を付して、署名付き電子文書を作成する。そして、作成した署名付き電子文書に鍵保持部12に保持されている公開鍵証明書を添付して、通信部16を介して、ユーザより指示された送信先のエンドエンティティEEのアドレスへ送信する。

【0031】

また、制御部18は、通信部16を介して、他のエンドエンティティEEから署名付き電子文書と公開鍵証明書を受け取ると、これらを検証対象保持部13に保持させると共に、その旨を署名検証部15に通知する。これを受けて、署名検証部15は、検証対象保持部13に保持されている署名付き電子文書の署名を、当該電子文書と共に受け取った公開鍵証明書を用いて検証する。そして、検証が成立した場合にのみ、署名付き電子文書を正当なものとして扱い、必要に応じて入出力部17から出力する。

【0032】

ただし、上記の署名検証が成立した場合でも、当該署名検証に用いた公開鍵証明書が、自エンドエンティティEEを収容する（つまり、自エンドエンティティEEに対して公開鍵証明書を発行した）端末収容認証局CA以外の端末収容認証局CAの場合は、証明書有効性確認センタVCに、上記の署名検証に用いた公開

鍵証明書の有効性の確認依頼を送信する。この際、必要に応じて、前記署名付き電子文書により行おうとしている電子手続の取引額等で示した信頼度（ポリシー）を、前記確認依頼に含める。そして、証明書有効性確認センタVCにて、当該公開鍵証明書の有効性が確認された場合にのみ、署名付き電子文書を正当なものとして扱い、必要に応じて入出力部17から出力する。

【0033】

次に、認証局CAについて説明する。

【0034】

図4は、認証局CAの概略構成を示す図である。

【0035】

図示するように、認証局CAは、処理部20aと、記憶部20bと、ネットワークNETを介して他装置と通信を行うための通信部26と、公開鍵証明書等の入出力やユーザよりの指示の受け付けを行う入出力部27と、を有する。

【0036】

処理部20aは、公開鍵証明書を発行する発行部21と、発行部21が発行した公開鍵証明書の管理を行う管理部22と、認証局CAの各部を統括的に制御する制御部28と、を有する。

【0037】

記憶部20bは、発行部21が発行した公開鍵証明書を保持する公開鍵証明書データベース23と、公開鍵証明書データベース23に保持されている各公開鍵証明書の発行先が記述された発行先管理リストを保持する発行先管理リスト保持部24と、失効証明書リスト保持部25と、を有する。

【0038】

このような構成において、制御部28は、入出力部27あるいは通信部26を介して、公開鍵証明書の発行依頼を受け付けると、その旨を発行部21に伝える。これを受けて、発行部21は、発行依頼主が署名生成に用いる秘密鍵（署名鍵）とこれに対する公開鍵証明書を作成する。この際、自認証局CAの秘密鍵で公開鍵証明書に署名をする。また、必要に応じて、公開鍵証明書中に、当該公開鍵証明書の有効期限や、信頼しない他の認証局の名称（Name Constrains）や、当該

公開鍵証明書の有効性確認のために許容される最大パス長（パス上の許容最大認証局数）や、電子手続の取引額等で表した当該公開鍵証明書と対の秘密鍵による署名の信頼度（ポリシー）を記述する。そして、作成した公開鍵証明書と秘密鍵を、入出力部 27 あるいは通信部 26 を介して、郵送あるいは通信により、発行依頼主に渡す。また、この公開鍵証明書を公開鍵証明書データベース 23 に登録すると共に、その発行先（つまり発行依頼主）の情報を、発行先管理リスト保持部 24 に保持されている発行先管理リストに記述する。

【0039】

また、制御部 28 は、入出力部 27 あるいは通信部 26 を介して、公開鍵証明書の失効依頼を受け付けると、その旨を管理部 22 に伝える。これを受けて、管理部 22 は、失効対象の公開鍵証明書を公開鍵証明書データベース 23 から削除すると共に、当該公開鍵証明書の発行先の情報を、発行先管理リスト保持部 24 に保持されている発行先管理リストから削除する。そして、管理部 22 は、失効依頼により公開鍵証明書データベース 23 から削除した公開鍵証明書に関する情報が記述された失効証明書リスト（一般に、CRL (Certification Revocation List)、ARL (Authority Revocation List) と呼ばれている）を、定期的に作成し、これを失効証明書リスト保持部 25 に保持させる。なお、管理部 22 は、作成した失効証明書リストに、次の失効証明書リストの作成予定日時を記述するものとする。

【0040】

また、制御部 28 は、通信部 26 を介して、他装置より公開鍵証明書の失効情報の問い合わせを受け取ると、失効証明書リスト保持部 25 に保持されている失効証明書リストを検索して、問い合わせのあった公開鍵証明書が失効しているか否かを調べる。そして、その結果を、通信部 26 を介して、問い合わせをした他装置に応答する（このような問い合わせと応答に用いる通信プロトコルとして、OSCP (Online Certification status protocol) がある）。

【0041】

なお、管理部 22 は、公開鍵証明書データベース 23 に格納されている各公開鍵証明書の有効期限を調査し、有効期限を過ぎている公開鍵証明書を公開鍵証明

書データベース23から削除すると共に、当該公開鍵証明書の発行先の情報を、発行先管理リスト保持部24に保持されている発行先管理リストから削除する処理も行う。

【0042】

次に、証明書有効性確認センタVCについて説明する。

【0043】

図5は、証明書有効性確認センタVCの概略構成を示す図である。

【0044】

図示するように、証明書有効性確認センタVCは、処理部30aと、記憶部30bと、ネットワークNETを介して他装置と通信を行うための通信部36と、公開鍵証明書等の入出力やユーザよりの指示の受け付けを行う入出力部37と、を有する。

【0045】

処理部30aは、パス検索部32と、パス検証部33と、有効期限/失効状態調査部34と、有効性確認部35と、証明書有効性確認センタVCの各部を統括的に制御する制御部38とを有する。また、記憶部30bは、パスデータベース31と、失効証明書リスト作成予定日時データベース39とを有する。

【0046】

パス検索部31は、定期的に、ブリッジ認証局CA_{bridge}からエンドエンティティEEに対して公開鍵証明書を発行した各端末収容認証局CAまでのパスを検索する。

【0047】

パス検証部32は、パス検索部31でパスの検索が行われる毎に、当該パス検索部31で検出されたパスの検証を行う。そして、検証が成立したパスを、証明書有効性確認センタVCを上流とした場合に当該パス上の最下流に位置することとなる端末収容認証局CAの名称と、当該パス上の各認証局CAから入手した当該パス上の1つ下流側に位置する認証局CA（発行元の認証局CAが端末収容認証局CAの場合はエンドエンティティEE）に対して発行した公開鍵証明書とに対応付けて、パスデータベース31に登録する。

【 0 0 4 8 】

有効期限/失効状態調査部 3 4 は、パスデータベース 3 1 に登録されているパス各々について、当該パス上の各認証局 C A が当該パス上の 1 つ下流側に位置する認証局 C A（発行元の認証局 C A が端末収容認証局 C A の場合はエンドエンティティ E E）に対して発行した公開鍵証明書の有効期限や失効の有無を調査する。そして、その結果に応じてパスデータベース 3 3 を更新する。

【 0 0 4 9 】

また、有効期限/失効状態調査部 3 4 は、各認証局 C A の失効証明書リスト保持部 2 5 から入手した失効証明書リストに記述されている次の失効証明書リスト作成予定日時を当該認証局 C A に対応付けて、失効証明書リスト作成予定日時データベース 3 9 に登録する。

【 0 0 5 0 】

有効性確認部 3 5 は、エンドエンティティ E E からの依頼に従い、当該エンドエンティティ E E を収容する端末収容認証局 C A 以外の端末収容認証局 C A が発行した公開鍵証明書の、当該エンドエンティティ E E を収容する端末収容認証局 C A に対する有効性の確認を行う。

【 0 0 5 1 】

なお、図 3 ～図 5 に示すエンドエンティティ E E、認証局 C A および証明書有効性確認センタ V C の各々は、例えば、図 6 に示すような、CPU 6 1 と、メモリ 6 2 と、ハードディスク等の外部記憶装置 6 3 と、CD-ROM等の可搬性を有する記憶媒体 6 9 から情報を読み取る読取装置 6 4 と、ネットワークを介して他装置と通信を行うための通信装置 6 5 と、キーボードやマウス等の入力装置 6 6 と、モニタやプリンタ等の出力装置 6 7 と、これらの各装置間のデータ送受を行うインターフェース 6 8 とを備えた、一般的な電子計算機において、CPU 6 1 がメモリ 6 2 上にロードされた所定のプログラムを実行することにより、実現できる。すなわち、通信部 1 6、2 6、3 6 は、CPU 6 1 が通信装置 6 6 を利用することにより、入出力部 1 7、2 7、3 7 は、CPU 6 1 が入力装置 6 6 や出力装置 6 7 や読取装置 6 4 を利用することにより、そして、記憶部 1 0 b、2 0 b、3 0 b は、CPU 6 1 がメモリ 6 2 や外部記憶装置 6 3 を利用することに

より実現される。また、処理部 1 0 a、2 0 a、3 0 a は、CPU 6 1 上のプロセスとして実現される。

【0 0 5 2】

このような、電子計算機上にエンドエンティティ E E、認証局 C A および証明書有効性確認センタ V C を各々実現するための所定のプログラムは、読取装置 6 4 を介して記憶媒体 6 9 から読み出され、あるいは、通信装置 6 6 を介してネットワーク経由で他のサーバからダウンロードされて、一旦、外部記憶装置 6 3 に格納された後、そこからメモリ 6 2 上にロードされて、あるいは、外部記憶装置 6 3 に格納されることなく、直接メモリ 6 2 上にロードされて、CPU 6 1 に実行されるようにすればよい。

【0 0 5 3】

次に、上記構成の証明書有効性確認センタ V C の動作について説明する。

【0 0 5 4】

本実施形態の証明書有効性確認センタ V C の動作は、パスの検索、検証および管理動作と、公開鍵証明書の有効性の確認動作とに分かれる。

【0 0 5 5】

まず、パスの検索・検証および管理動作について説明する。

【0 0 5 6】

図 7 ～ 図 8 は、本実施形態の証明書有効性確認センタ V C で行われるパスの検索、検証および管理動作を説明するためのフロー図である。

【0 0 5 7】

制御部 3 8 は、所定時間（例えば 1 日）を経過すると（ステップ S 1 0 0 1）、パス検索部 3 2 にパス検索を依頼する。これを受けて、パス検索部 3 2 は、ブリッジ認証局 C A_{bridge} から各端末収容認証局 C A までのパスを検索する（ステップ S 1 0 0 2）。

【0 0 5 8】

具体的には、パス検索部 3 2 は、ブリッジ認証局 C A_{bridge} の発行先管理リスト保持部 2 4 にアクセスし、ブリッジ認証局 C A_{bridge} が発行した公開鍵証明書の発行先の情報を入手する。そして、入手した各発行先が認証局 C A の場合は、

各発行先の認証局CAの発行先管理リスト保持部24にアクセスして、各認証局CAが発行した公開鍵証明書の発行先をさらに調べる。この処理を、公開鍵証明書の発行先がエンドエンティティEEとなるまで続けることにより、ブリッジ認証局CA_{bridge}から各端末収容認証局CAまでのパスを検索する。ここで、パスのループにより上記の処理が無限に繰り返されるのを防止するため、ある認証局CAの発行先管理リスト保持部24から入手した発行先に、それまでに形成された部分パスの上流側に位置する認証局CAが含まれる場合は、当該認証局CAを発行先とした上記の処理を行わないものとする。

【0059】

ステップS1002でのパス検索処理を、各認証局CAが図2に示す関係にある場合を例に取り、より具体的に説明する。

【0060】

まず、パス検索部32は、ブリッジ認証局CA_{bridge}の発行先管理リスト保持部24にアクセスし、ブリッジ認証局CA_{bridge}が発行した公開鍵証明書の発行先の情報として、認証局CA₁₁、CA₂₁、CA₃₁の情報を入手する。

【0061】

次に、パス検索部32は、ブリッジ認証局CA_{bridge}から入手した発行先（認証局CA₁₁、CA₂₁、CA₃₁）のうちのいずれか1つに注目して、以下の処理を実行する。

【0062】

すなわち、注目した発行先が認証局CA（以下、注目認証局CAと呼ぶこととする）であるならば、ブリッジ認証局CA_{bridge}-注目認証局CA間に、ブリッジ認証局CA_{bridge}側を上流とする部分パスを設定する。そして、注目認証局CAの発行先管理リスト保持部24にアクセスして、当該注目認証局CAが発行した公開鍵証明書の発行先の情報をさらに入手する。ここでは、注目した発行先が認証局CA₁₁であるとして、ブリッジ認証局CA_{bridge}-認証局CA₁₁間に部分パスを設定し、認証局CA₁₁から、発行先の情報として、認証局CA_{bridge}、CA₁₂、CA₁₃の情報を入手したものとする。

【0063】

次に、パス検索部 3 2 は、認証局 CA_{11} から入手した発行先（認証局 CA_{bridge} 、 CA_{12} 、 CA_{13} ）に、部分パス上の認証局 CA （以下、ループ認証局 CA と呼ぶこととする）が含まれているか否かを調べる。含まれている場合はその発行先を注目対象から除外する。したがって、ここでは、認証局 CA_{bridge} を注目対象から除外することになる。次に、パス検索部 3 2 は、認証局 CA_{11} から入手した発行先にエンドエンティティ EE が含まれるか否かを調べる。エンドエンティティ EE が含まれている場合、認証局 CA_{11} は端末収容認証局となる。しかし、認証局 CA_{11} から入手した発行先にエンドエンティティ EE は含まれていない。したがって、ブリッジ認証局 CA_{bridge} -認証局 CA_{11} 間に設定した部分パスを、端末収容認証局 CA まで延長すべく、認証局 CA_{11} から入手した、ループ認証局 CA を除く発行先（認証局 CA_{12} 、 CA_{13} ）のうちのいずれか 1 つに注目する。

【 0 0 6 4 】

注目した発行先が認証局 CA であるならば、それまでに設定した部分パスの下流側にこの注目認証局 CA を接続した部分パスを設定する。そして、この注目認証局 CA の発行先管理リスト保持部 2 4 にアクセスして、当該注目認証局 CA が発行した公開鍵証明書の発行先の情報をさらに入手する。ここでは、注目した発行先が認証局 CA_{12} であるとして、ブリッジ認証局 CA_{bridge} -認証局 CA_{11} -認証局 CA_{12} 間に部分パスを設定し、認証局 CA_{12} から、発行先の情報として、エンドエンティティ EE_1 、 EE_2 を入手したものとする。

【 0 0 6 5 】

次に、パス検索部 3 2 は、認証局 CA_{12} から入手した発行先（ EE_1 、 EE_2 ）に、ループ認証局 CA が含まれているか否かを調べる。含まれている場合はその発行先を注目対象から除外する。ここでは、ループ認証局 CA は含まれないので、パス検索部 3 2 は、次の処理へ移行し、端末収容認証局 CA_{12} から入手した発行先にエンドエンティティ EE が含まれるか否かを調べる。ここで、入手した発行先はすべてエンドエンティティ EE であるので、認証局 CA_{12} は端末収容認証局である。そこで、この認証局 CA_{12} を最下流とする部分パスを、ブリッジ認証局 CA_{bridge} から端末収容認証局 CA_{12} までのパス（ CA_{bridge} - CA_{11} - CA_{12} ）として検出する。

【 0 0 6 6 】

次に、パス検索部 3 2 は、検出したパス上の最下流側に位置する認証局 CA_{12} から入手した発行先の情報の中に、未だ注目していない発行先（ループ認証局 CA 以外の認証局 CA ）があるか否かを調べ、そのような発行先があれば、これを注目認証局 CA として、上記の処理を続ける。一方、そのような発行先がなければ、1 つ上流側に位置する認証局 CA_{11} から入手した発行先の情報の中に、未だ注目していない発行先（ループ認証局 CA 以外の認証局 CA ）があるか否かを調べる。そして、そのような発行先があれば、これを注目認証局 CA として、上記の処理を続ける。ここでは、認証局 CA_{11} から入手した発行先の情報のうち、認証局 CA_{13} について未だ注目していないので、これを注目認証局 CA として上記の処理を行うことにより、ブリッジ認証局 CA_{bridge} から端末収容認証局 CA_{13} までのパス（ $CA_{bridge}-CA_{11}-CA_{13}$ ）を検出する。

【 0 0 6 7 】

このように、パス検索部 3 2 は、上記の処理を、検出したパス上に位置する全ての認証局 CA 各々について、当該認証局 CA から入手した発行先の情報の中に、未だ注目していない発行先（ループ認証局 CA 以外の認証局 CA ）がなくなるまで続けることにより、ブリッジ認証局 CA_{bridge} から各端末収容認証局 CA までのパスを検出する。その結果、各認証局 CA が図 2 に示す関係にある場合、パス検索部 3 2 により検出される、ブリッジ認証局 CA_{bridge} から各端末収容認証局 CA までのパスは、図 9 に示すとおりとなる。

【 0 0 6 8 】

さて、制御部 3 8 は、パス検索部 3 2 によりブリッジ認証局 CA_{bridge} から各端末収容認証局 CA までのパスが検出されると、パス検証部 3 3 にパスの検証を依頼する。これを受けて、パス検証部 3 3 は、パス検索部 3 2 により検出されたパスの検証を行う（ステップ S 1 0 0 3）。

【 0 0 6 9 】

具体的には、パス検索部 3 2 により検出されたパス各々について、以下の処理を行う。

【 0 0 7 0 】

すなわち、まず、パス検証部 3 3 は、パス上の各認証局 C A の公開鍵証明書データベース 2 3 にアクセスし、各認証局 C A が当該パス上の 1 つ下流側に位置する認証局 C A (アクセス先認証局 C A が端末認証局 C A の場合はエンドエンティティ E E) に対して発行した公開鍵証明書を入手する。

【 0 0 7 1 】

次に、パス検証部 3 3 は、パスの最下流に位置する端末収容認証局 C A が発行した公開鍵証明書の署名を、1 つ上流側の認証局 C A が発行した公開鍵証明書で検証し、検証が成立した場合は当該 1 つ上流側の認証局 C A が発行した公開鍵証明書の署名をさらに 1 つ上流側の認証局 C A が発行した公開鍵証明書で検証する。この処理を、当該 1 つ上流側の認証局 C A がブリッジ認証局 C A_{bridge} となるまで続けることにより、当該パスを仮検証する。

【 0 0 7 2 】

例えば、図 2 においてブリッジ認証局 C A_{bridge} から端末収容認証局 C A₁₃ までのパス (C A_{bridge}-C A₁₁-C A₁₃) を仮検証する場合、まず、端末収容認証局 C A₁₃ が発行した公開鍵証明書の署名を、端末収容認証局 C A₁₃ より 1 つ上流側の認証局 C A であるルート認証局 C A₁₁ が端末収容認証局 C A₁₃ に対して発行した公開鍵証明書を用いて検証する。そして、検証が成立した場合は、ルート認証局 C A₁₁ が発行した公開鍵証明書の署名を、ルート認証局 C A₁₁ より 1 つ上流側の認証局 C A であるブリッジ認証局 C A_{bridge} がルート認証局 C A₁₁ に対して発行した公開鍵証明書を用いて検証する。そして、この検証が成立した場合に、ブリッジ認証局 C A_{bridge} から端末収容認証局 C A₁₃ までのパスの仮検証が成立したものとする。

【 0 0 7 3 】

次に、パス検証部 3 3 は、パスの仮検証が成立したならば、当該パス上の各認証局 C A から入手した公開鍵証明書中に、信頼しない他の認証局の名称 (Name Constraints) や当該公開鍵証明書の有効性確認のために許容される最大パス長 (パス上の許容最大認証局数) などの制限の記述があるか否かを調べる。そのような記述がある場合は、当該パスがその制限を満たしているか否かを調べ、満たしている場合にのみ、当該パスの検証が成立したものとする。

【 0 0 7 4 】

例えば、図 2 においてブリッジ認証局 CA_{bridge} から端末収容認証局 CA_{26} までのパス ($CA_{bridge}-CA_{31}-CA_{21}-CA_{22}-CA_{25}-CA_{26}$) の仮検証が成立した場合において、認証局 CA_{26} から入手した公開鍵証明書中に信頼しない他の認証局の名称として認証局 CA_{31} が記述されている場合、当該パスの検証は成立しなかったものとする。また、上記の場合において、認証局 CA_{26} から入手した公開鍵証明書中にパス長として認証局数 = 5 が記述されている場合、当該パスの検証は成立しなかったものとする。

【 0 0 7 5 】

さて、制御部 38 は、上記のようにして、パス検索部 32 により検出されたパス各々に対するパス検証部 33 での検証が終了したならば、パスデータベース 31 の登録内容を一旦クリアし、それから、パス検証部 33 での検証が成立したパス各々を、当該パス上の最下流に位置する端末収容認証局 CA と、当該パス上の各認証局 CA から入手した公開鍵証明書とに対応付けて、パスデータベース 31 に登録する (ステップ S1004)。

【 0 0 7 6 】

一方、有効期限/失効状態調査部 34 は、パスデータベース 31 に登録されている公開鍵証明書の中に、有効期限切れの公開鍵証明書があるか否かを調べる (ステップ S1005)。有効期限切れの公開鍵証明書がある場合は、当該公開鍵証明書の発行元認証局 CA の公開鍵証明書データベース 23 にアクセスして、当該公開鍵証明書の発行先に対して新たに発行された公開鍵証明書を検索する (ステップ S1006)。

【 0 0 7 7 】

そして、そのような公開鍵証明書が前記発行元認証局 CA の公開鍵証明書データベース 23 中になければ、前記有効期限切れの公開鍵証明書に対応付けて登録されているパスに関する情報をパスデータベース 31 から削除する (ステップ S1007)。一方、そのような公開鍵証明書が前記発行元認証局 CA の公開鍵証明書データベース 23 中にあればこれを入手する。そして、前記有効期限切れの公開鍵証明書に対応付けてパスデータベース 31 に登録されているパスの検証を

、当該有効期限切れの公開鍵証明書の代わりに新たに入手した公開鍵証明書を用いて、上記のステップ S 1 0 0 3 と同じ要領で行う（ステップ S 1 0 0 8）。

【 0 0 7 8 】

なお、ステップ S 1 0 0 8 でのパス検証に代えて、新たに入手した公開鍵証明書の署名を、当該パス上において、当該公開鍵証明書の発行元認証局 C A より 1 つ上流側に位置する認証局 C A が発行した公開鍵証明書で検証し、検証が成立した場合に、当該パスの検証が成立したものとして扱うようにしてもよい。

【 0 0 7 9 】

さて、パスの検証が成立した場合（ステップ S 1 0 0 9 で Y e s）は、当該パスに対応付けられてパスデータベース 3 1 に登録されている前記有効期限切れの公開鍵証明書を、新たに入手した公開鍵証明書に置き換える（ステップ S 1 0 1 0）。一方、パスの検証が成立しなかった場合（ステップ S 1 0 0 9 で N o）は、前記有効期限切れの公開鍵証明書に対応付けて登録されているパスをパスデータベース 3 1 から削除する（ステップ S 1 0 1 1）。

【 0 0 8 0 】

次に、有効期限/失効状態調査部 3 4 は、失効証明書リスト作成予定日時データベース 3 9 を調べ、既に経過した失効証明書リスト作成予定日時に対応付けられている認証局 C A を検索する（ステップ S 1 0 1 2）。そのような認証局 C A が存在する場合（ステップ S 1 0 1 3 で Y e s）は、当該認証局 C A の失効証明書リスト保持部 2 5 にアクセスして、当該認証局 C A が発行した最新の失効証明書リストを入手する（ステップ S 1 0 1 4）。そして、失効証明書リスト作成予定日時データベース 3 9 にて、当該認証局 C A に対応付けて登録されている失効証明書リスト作成予定日時を、入手した最新の失効証明書リストに記述されている失効証明書リスト作成予定日時に更新する（ステップ S 1 0 1 5）。

【 0 0 8 1 】

それから、有効期限/失効状態調査部 3 4 は、入手した最新の失効証明書リストに記述されている公開鍵証明書が、パスデータベース 3 1 に登録されているか否かを調べ（ステップ S 1 0 1 6）、登録されている場合は、当該公開鍵証明書に対応付けられているパスに関する情報をパスデータベース 3 1 から削除する（

ステップ S 1 0 1 7)。

【 0 0 8 2 】

次に、公開鍵証明書の有効性の確認動作について説明する。

【 0 0 8 3 】

図 1 0 ～ 図 1 1 は、本実施形態の証明書有効性確認センタ V C で行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【 0 0 8 4 】

制御部 3 8 は、通信部 3 6 を介して、エンドエンティティ E E から、少なくとも当該エンドエンティティ E E を収容する端末収容認証局 C A の名称を含んだ、当該端末収容認証局 C A 以外の端末収容認証局 C A が発行した公開鍵証明書の有効性の確認依頼を受け取ると（ステップ S 2 0 0 1）、その旨を有効性確認部 3 5 に通知する。

【 0 0 8 5 】

これを受けて、有効性確認部 3 5 は、依頼対象の公開鍵証明書の記述から特定される当該証明書を発行した端末収容認証局 C A に対応付けられたパスと、依頼主のエンドエンティティ E E を収容する端末収容認証局 C A に対応付けられたパスとが、パスデータベース 3 1 に登録されているか否かを調べる（ステップ S 2 0 0 2）。

【 0 0 8 6 】

その結果、依頼対象の公開鍵証明書を発行した端末収容認証局 C A に対応付けられたパス、および、依頼主のエンドエンティティ E E を収容する端末収容認証局 C A に対応付けられたパスの両方が、パスデータベース 3 1 に登録されていないことが判明したならば、有効性確認部 3 5 は、公開鍵証明書が有効でない旨を、通信部 3 6 を介して、依頼主のエンドエンティティ E E に通知する（ステップ S 2 0 0 3）。

【 0 0 8 7 】

一方、依頼対象の公開鍵証明書を発行した端末収容認証局 C A に対応付けられたパス、および、依頼主のエンドエンティティ E E を収容する端末収容認証局 C A に対応付けられたパスの両方が、パスデータベース 3 1 に登録されていること

が確認できたならば、有効性確認部35は、これら2つのパスのいずれかに対応付けられてパスデータベース31に登録されている各公開鍵証明書中に、信頼しない他の認証局の名称 (Name Constrains) や当該公開鍵証明書の有効性確認のために許容される最大パス長 (パス上の許容最大認証局数) などの制限の記述があるか否かをさらに調べる (ステップS2004)。

【0088】

そのような制限の記述がない場合、ステップS2006に移行する。一方、そのような制限の記述がある場合は、ステップS2005に移行して、これら2つのパスがその制限を満たしているか否か、すなわち、各公開鍵証明書中に、これら2つのパス上のいずれかの認証局を信頼しない旨が記述されているか否か、および、最大パス長として、これら2つのパス上の認証局数よりも少ない認証局数が記述されているか否かを調べる。

【0089】

そして、そのような記述がある場合、有効性確認部35は、これら2つのパスがその制限を満たしていないものと判断し、公開鍵証明書が有効性でない旨を、通信部36を介して、依頼主のエンドエンティティEEに通知する (ステップS2003)。一方、そのような記述がない場合は、これら2つのパスがその制限を満たしているものと判断し、ステップS2006に移行する。

【0090】

ステップS2006では、有効性確認部35は、エンドエンティティEEから受け取った確認依頼に、当該エンドエンティティEEが行おうとしている電子手続の取引額等で示された信頼度 (ポリシー) が含まれているか否かを調べる。電子手続の信頼度が含まれている場合は、これら2つのパスのいずれかに対応付けられてパスデータベース31に登録されている各公開鍵証明書中に、前記電子手続の信頼度よりも低い信頼度の記述があるか否かをさらに調べる (ステップS2007)。

【0091】

そして、そのような記述がある場合は、これら2つのパスを、依頼主のエンドエンティティEEが行おうとしている電子手続のための公開鍵証明書の有効性確

認に利用できないものと判断し、公開鍵証明書が有効でない旨を、通信部 3 6 を介して、依頼主のエンドエンティティ E E に通知する（ステップ S 2 0 0 3）。

【 0 0 9 2 】

一方、エンドエンティティ E E から受け取った確認依頼に当該エンドエンティティ E E が行おうとしている電子手続の信頼度が含まれていない場合、あるいは、含まれていても、これら 2 つのパスのいずれかに対応付けられてパスデータベース 3 1 に登録されている各公開鍵証明書中に記述されている信頼度が前記電子手続の信頼度よりも高い場合は、公開鍵証明書は有効であると判断し、公開鍵証明書が有効である旨を、通信部 3 6 を介して、依頼主のエンドエンティティ E E に通知する（ステップ S 2 0 0 8）。

【 0 0 9 3 】

以上、本発明の第 1 実施形態について説明した。

【 0 0 9 4 】

本実施形態では、ブリッジ認証局 C A_{bridge} から各端末収容認証局 C A までのパスの検索および検証を、エンドエンティティ E E からの公開鍵証明書の有効性確認依頼とは独立して、定期的に行うようにしている。そして、あるエンドエンティティ E E から公開鍵証明書の有効性確認依頼を受けた場合、予め検索、検証したパスを用いて、当該エンドエンティティ E E を収容する端末収容認証局 C A と依頼対象の公開鍵証明書を発行した端末収容認証局 C A との間に、ブリッジ認証局 C A_{bridge} を介したパスを構築することができるか否かを調べることで、当該公開鍵証明書が有効であるか否かを判断するようにしている。したがって、公開鍵証明書の有効性確認依頼を受けてから、当該有効性を確認するまでにかかる時間を短縮することができる。

【 0 0 9 5 】

また、本実施形態では、あるエンドエンティティ E E から公開鍵証明書の有効性確認依頼を受けた場合、予め検索、検証したパスを用いて、当該エンドエンティティ E E を収容する端末収容認証局 C A と依頼対象の公開鍵証明書を発行した端末収容認証局 C A との間に、ブリッジ認証局 C A_{bridge} を介したパスを構築することができるか否かを調べ、できた場合に、当該パス上の認証局が発行した公

開鍵証明書中に記述された制限（信頼しない他の認証局の名称（Name Constraints）や最大パス長（パス上の許容最大認証局数）や信頼度（ポリシー）等）を考慮して、依頼対象の公開鍵証明書が有効であるか否かを最終的に判断するようにしている。したがって、公開鍵証明書の有効性確認の判断をより正確に行うことが可能となる。

【 0 0 9 6 】

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【 0 0 9 7 】

例えば、上記の実施形態では、証明書有効性確認センタ VC は、ブリッジ認証局 CA_{bridge} を起点認証局とし、ブリッジ認証局 CA_{bridge} から各端末収容認証局 CA までのパスの検索および検証を行うようにしている。しかし、本発明はこれに限定されない。他の任意の認証局 CA を起点認証局として、各端末収容認証局 CA までのパスの検索および検証を行うこともできる。例えば、各認証局 CA が図 2 に示す関係にある場合、各セキュリティドメイン SD のルート認証局 CA₁₁、CA₂₁、CA₃₁ のいずれかを起点認証局として、各端末収容認証局 CA までのパスの検索および検証を行うようにしてもよい。

【 0 0 9 8 】

また、上記の実施形態では、説明をわかりやすくするため、図 2 に示すように、端末収容認証局 CA はエンドエンティティ EE に対してのみ公開鍵証明書を発行し、その他の認証局 CA は認証局 CA に対してのみ公開鍵証明書を発行するものとしているが、本発明は、当然のことながら、エンドエンティティ EE と認証局 CA の両方に対して公開鍵証明書を発行するような認証局 CA を含む場合でも、同様に適用できる。

【 0 0 9 9 】

【発明の効果】

以上説明したように、本発明によれば、公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短縮することができる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態が適用された P K I システムの概略構成を示す図である。

【図 2】

図 1 に示す P K I システムでの各認証局 C A の関係の一例を示す図である。

【図 3】

図 1 に示すエンドエンティティ E E の概略構成を示す図である。

【図 4】

図 1 に示す認証局 C A の概略構成を示す図である。

【図 5】

図 1 に示す証明書有効性確認センタ V C の概略構成を示す図である。

【図 6】

図 3 ～図 5 に示すエンドエンティティ E E 、 認証局 C A および証明書有効性確認センタ V C の各々のハードウェア構成例を示す図である。

【図 7】

図 5 に示す証明書有効性確認センタ V C で行われるパスの検索、検証および管理動作を説明するためのフロー図である。

【図 8】

図 5 に示す証明書有効性確認センタ V C で行われるパスの検索、検証および管理動作を説明するためのフロー図である。

【図 9】

各認証局 C A が図 2 に示す関係にある場合に、証明書有効性確認センタ V C のパス検索部 3 2 で検出される、ブリッジ認証局 C A_{bridge} から各端末収容認証局 C A までのパスを示す図である。

【図 1 0】

図 5 に示す証明書有効性確認センタ V C で行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【図 1 1】

図 5 に示す証明書有効性確認センタ V C で行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【図 1 2】

従来の P K I において、認証局が複数ある場合における各認証局の関係の一例を示す図である。

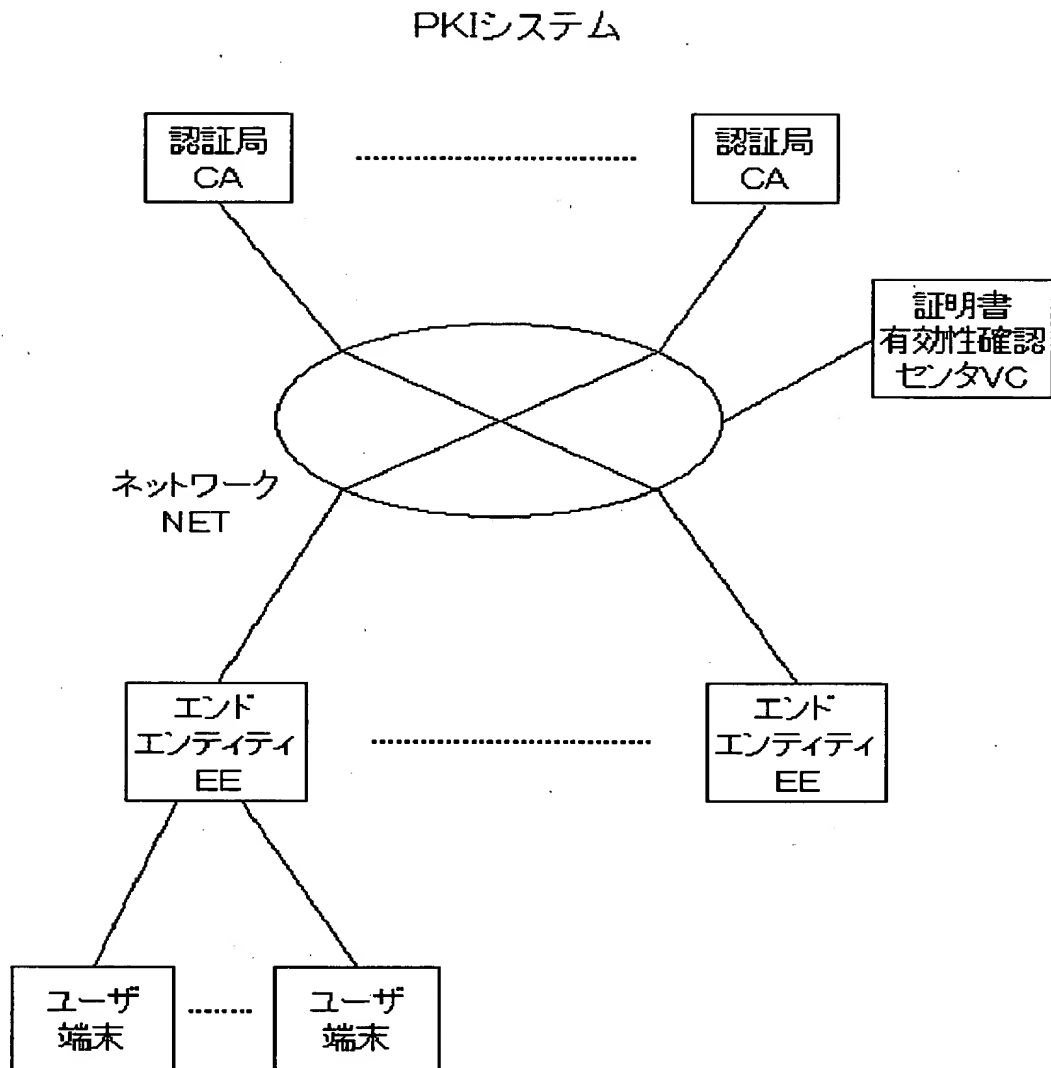
【符号の説明】

CA…認証局、VC…証明書有効性確認センタ、EE…エンドエンティティ、SD…セキュリティドメイン、10a, 20a, 30a…処理部、10b, 20b, 30b…記憶部、11…電子文書保持部、12…鍵保持部、13…検証対象保持部、14…署名生成部、15…署名検証部、16, 26, 36…通信部、17, 27, 37…入出力部、18, 28, 38…制御部、21…発行部、22…管理部、23…公開鍵証明書データベース、24…発行先リスト保持部、25…失効証明書リスト保持部、31…パスデータベース、32…パス検索部、33…パス検証部、34…有効期限/失効状態調査部、35…有効性確認部、39…失効証明書リスト作成予定日時データベース、61…CPU、62…メモリ、63…外部記憶装置、64…読取装置、65…通信装置、66…入力装置、67…出力装置、68…インターフェース、69…記憶媒体

【書類名】図面

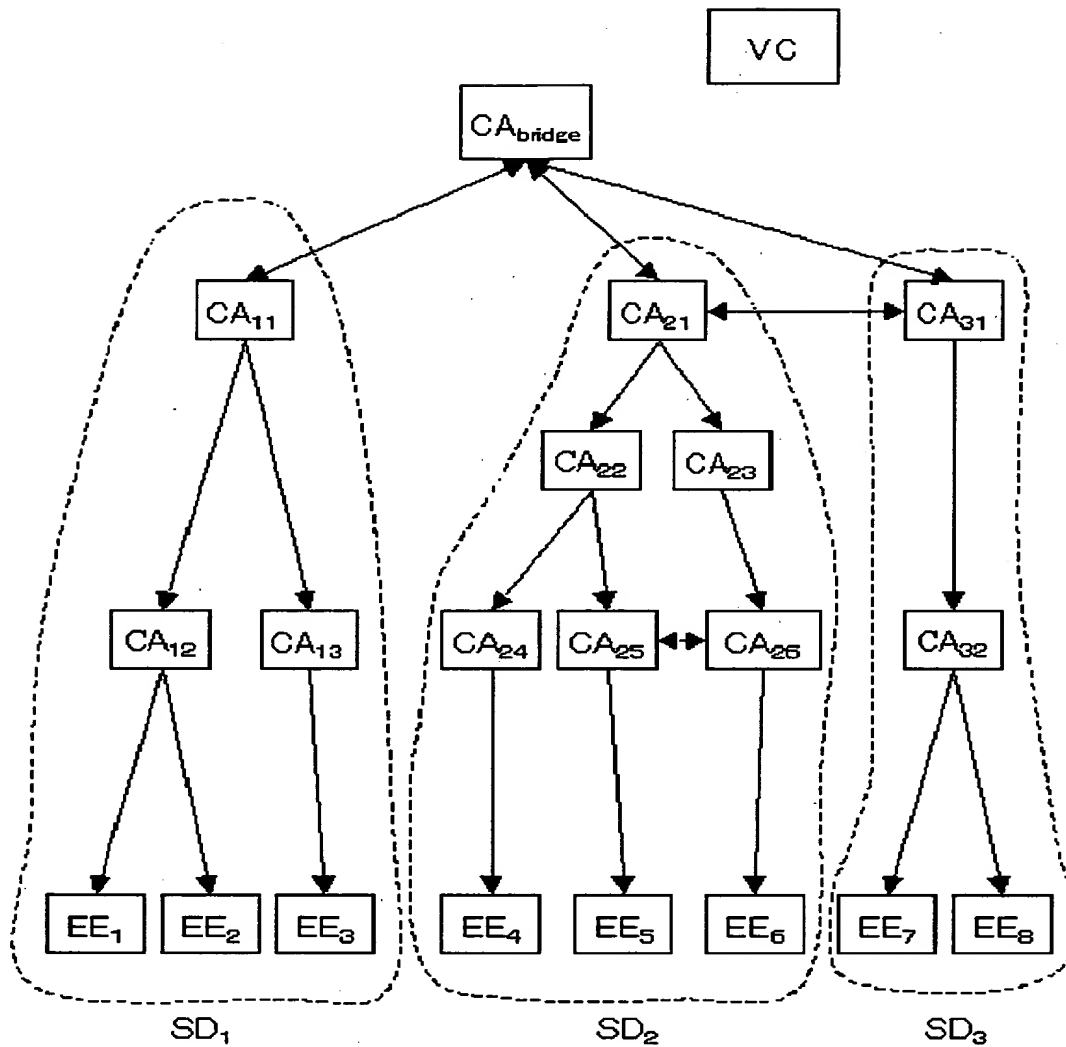
【図1】

図1



【図2】

図2



→ : 公開鍵証明書の流れ

CA: 認証局

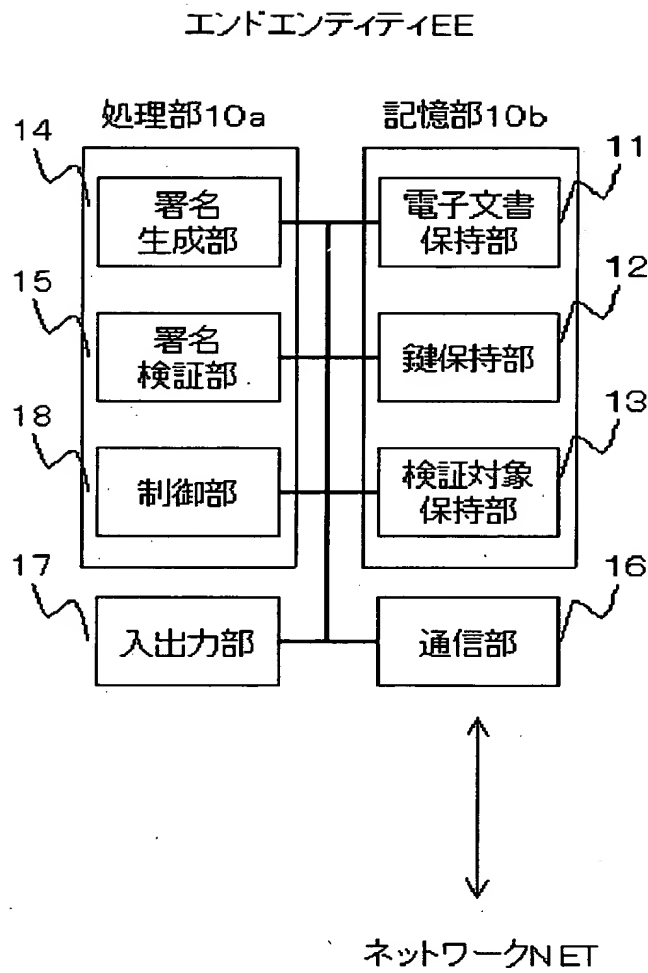
EE: エンドエンティティ

VC: 証明書有効性確認センタ

SD: セキュリティドメイン

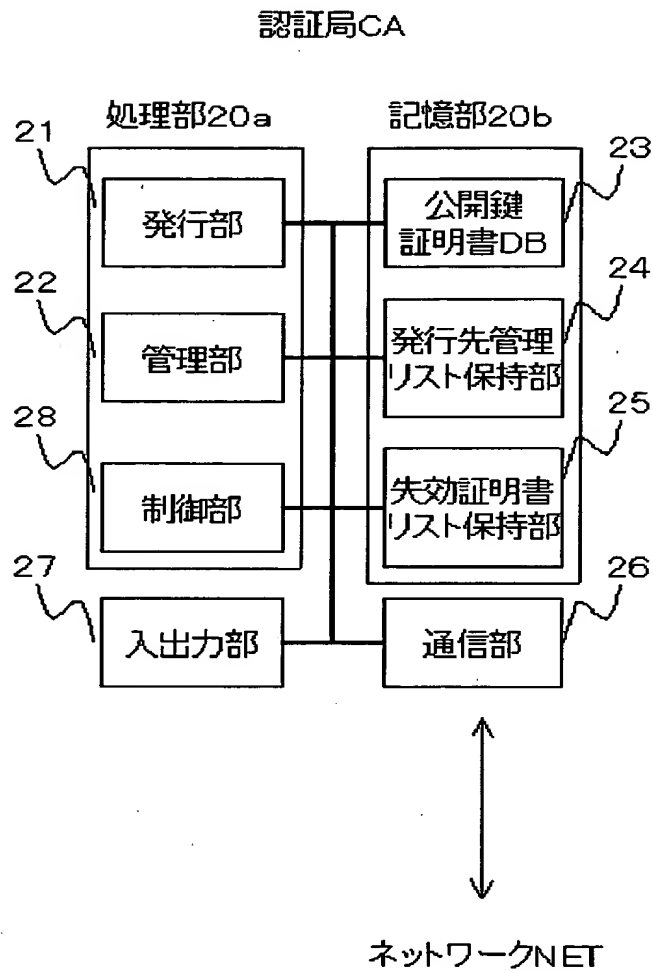
【図 3】

図 3



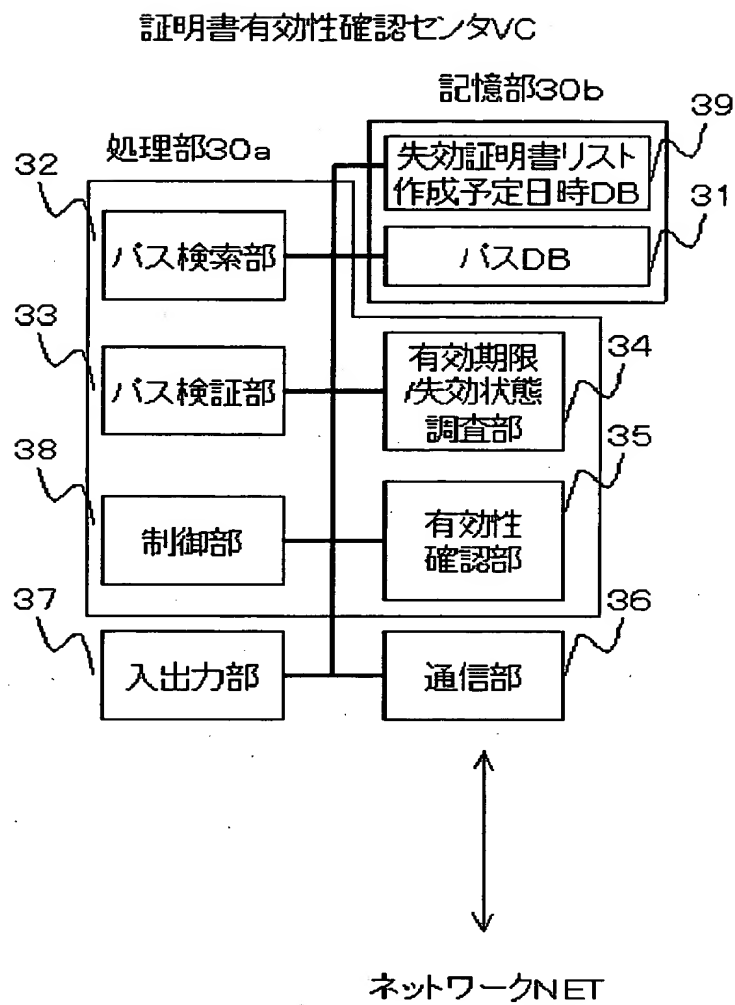
【図 4】

図 4



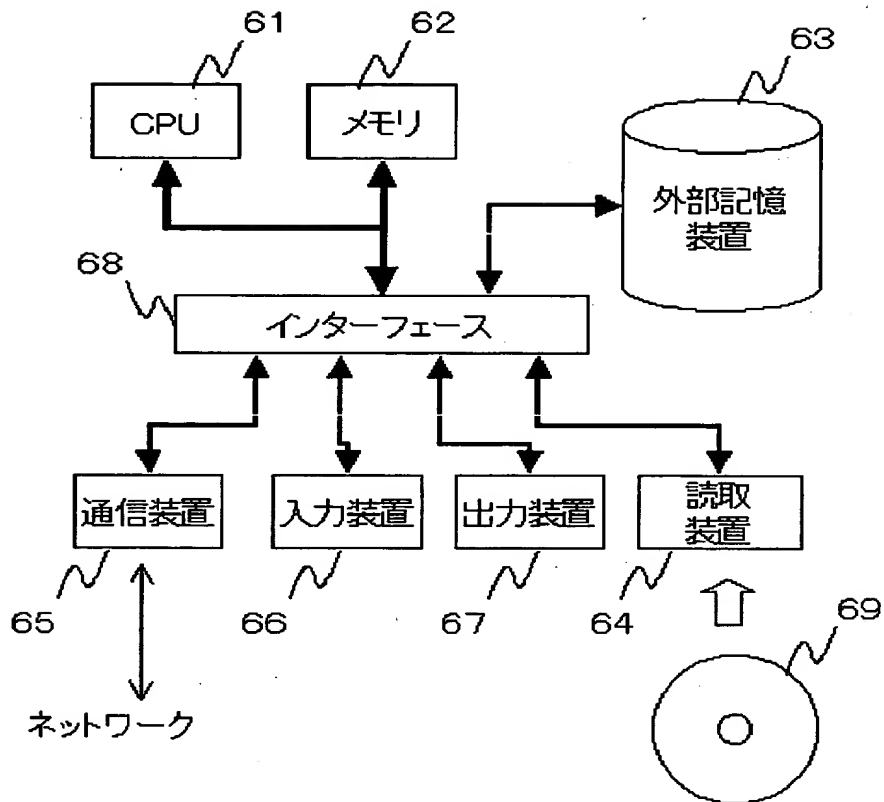
【図 5】

図 5



【図 6】

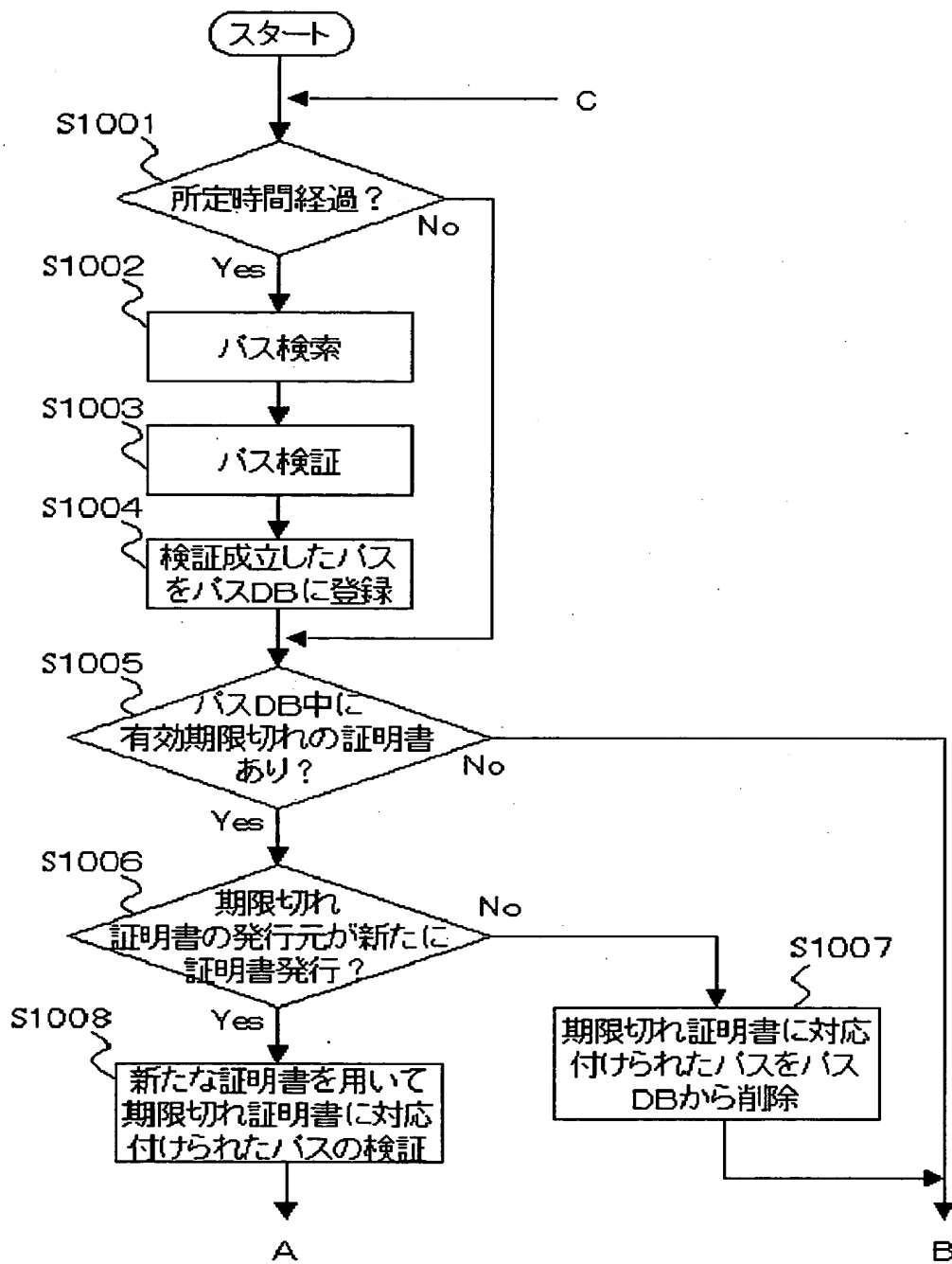
図 6



【図 7】

図 7

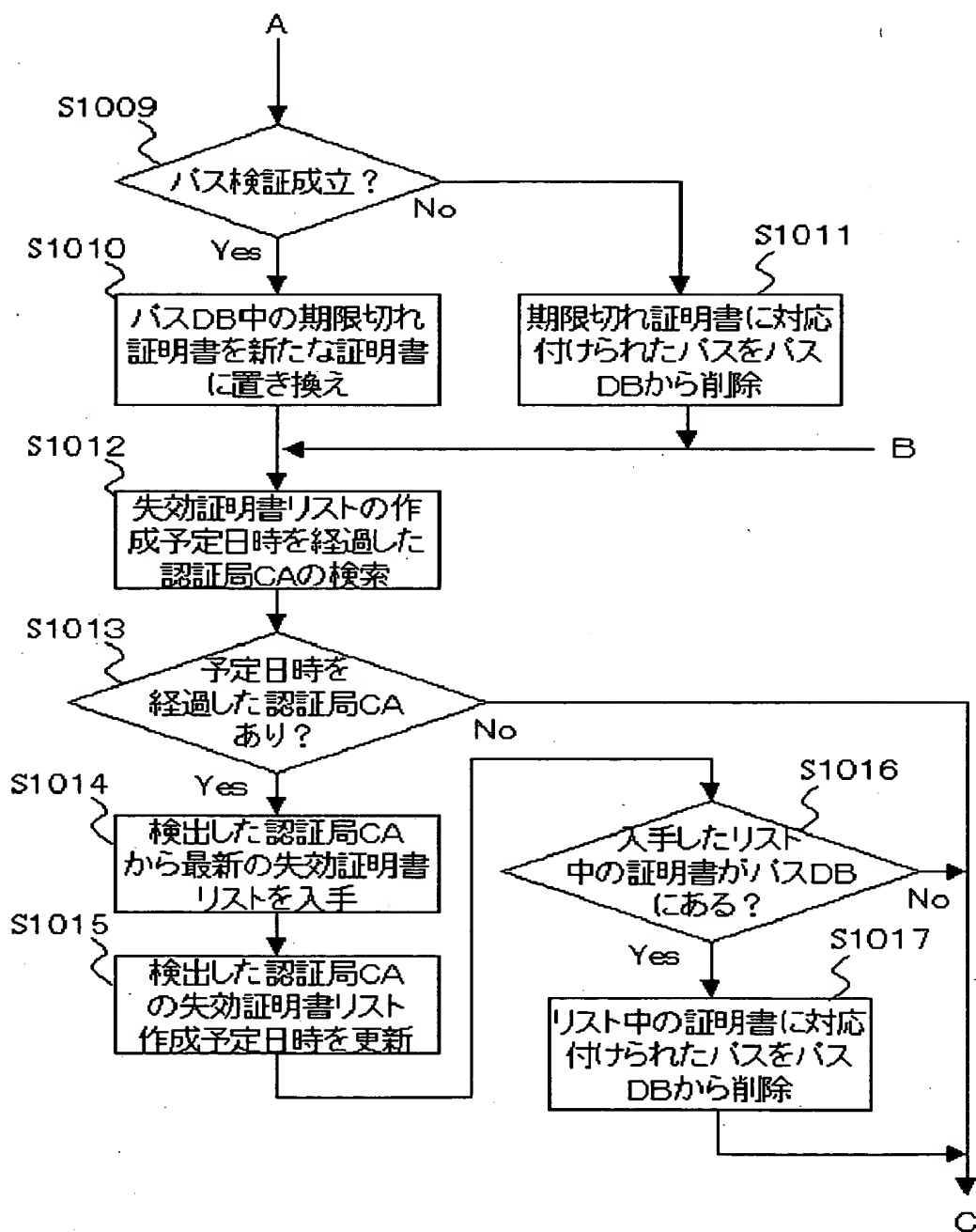
バスの検索、検証および管理動作



【図8】

図8

バスの検索、検証および管理動作



【図 9】

図 9

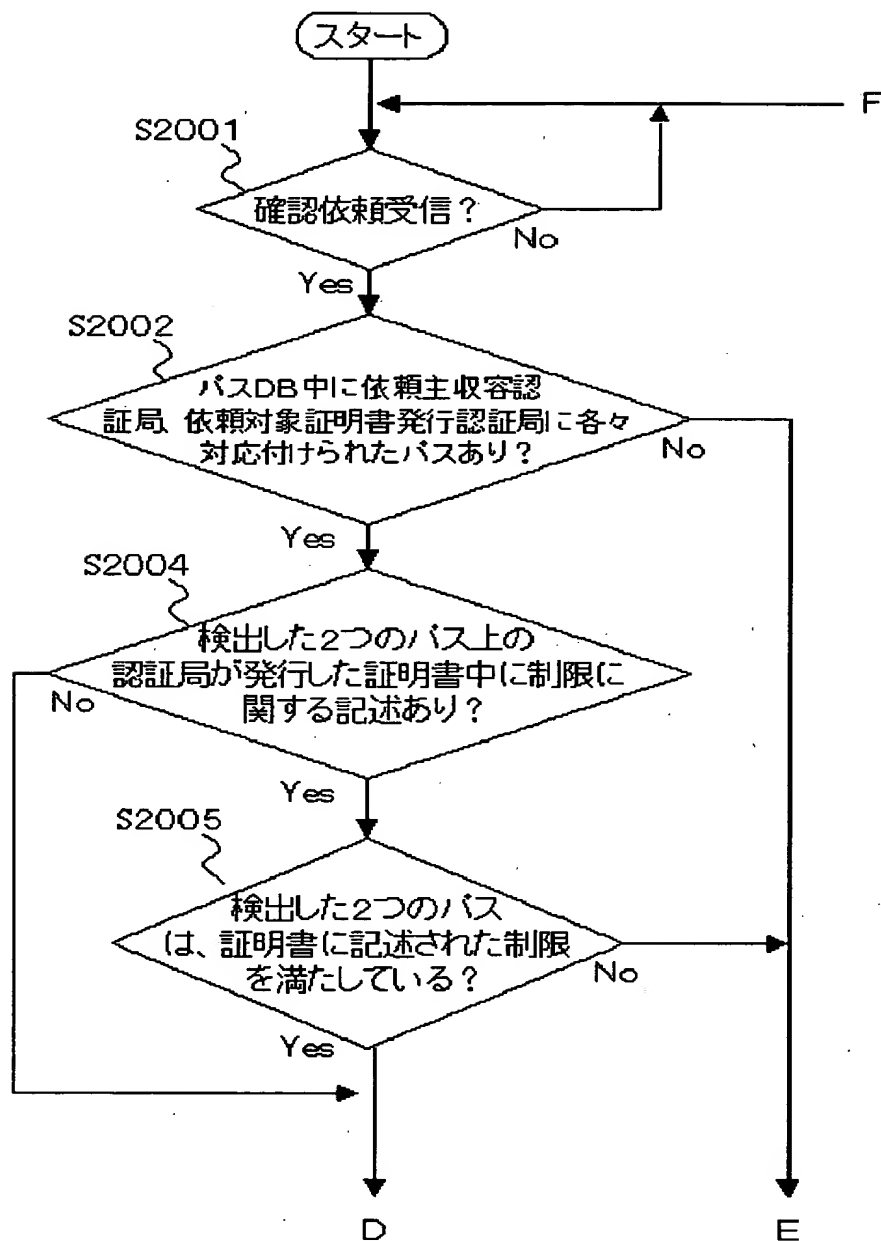
バス検索結果 (図 2 の場合)

端末収容認証局	バス
CA ₁₂	CA _{bride} -CA ₁₁ -CA ₁₂
CA ₁₃	CA _{bride} -CA ₁₁ -CA ₁₃
CA ₂₄	CA _{bride} -CA ₂₁ -CA ₂₂ -CA ₂₄
	CA _{bride} -CA ₃₁ -CA ₂₁ -CA ₂₂ -CA ₂₄
CA ₂₅	CA _{bride} -CA ₂₁ -CA ₂₂ -CA ₂₅
	CA _{bride} -CA ₂₁ -CA ₂₃ -CA ₂₆ -CA ₂₅
	CA _{bride} -CA ₃₁ -CA ₂₁ -CA ₂₂ -CA ₂₅
	CA _{bride} -CA ₃₁ -CA ₂₁ -CA ₂₃ -CA ₂₆ -CA ₂₅
CA ₂₆	CA _{bride} -CA ₂₁ -CA ₂₃ -CA ₂₆
	CA _{bride} -CA ₂₁ -CA ₂₂ -CA ₂₅ -CA ₂₆
	CA _{bride} -CA ₃₁ -CA ₂₁ -CA ₂₃ -CA ₂₆
	CA _{bride} -CA ₃₁ -CA ₂₁ -CA ₂₂ -CA ₂₅ -CA ₂₆
CA ₃₂	CA _{bride} -CA ₃₁ -CA ₃₂
	CA _{bride} -CA ₂₁ -CA ₃₁ -CA ₃₂

【図10】

図10

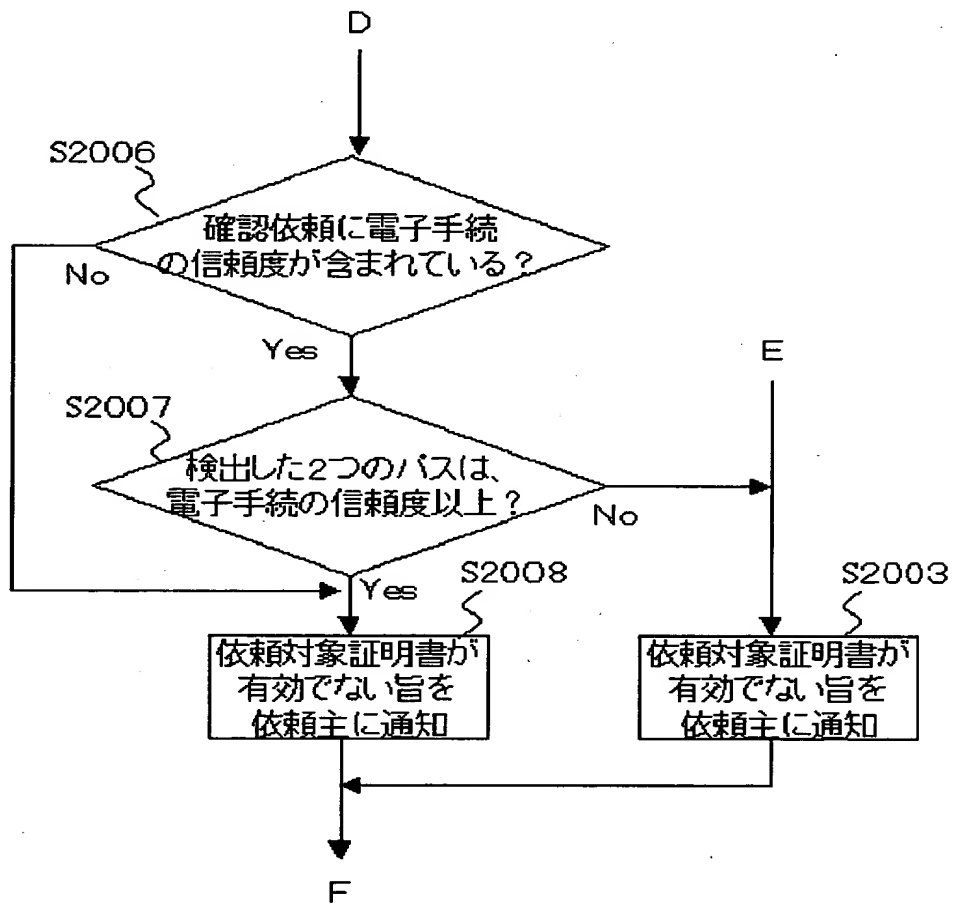
公開鍵証明書の有効性の確認動作



【図11】

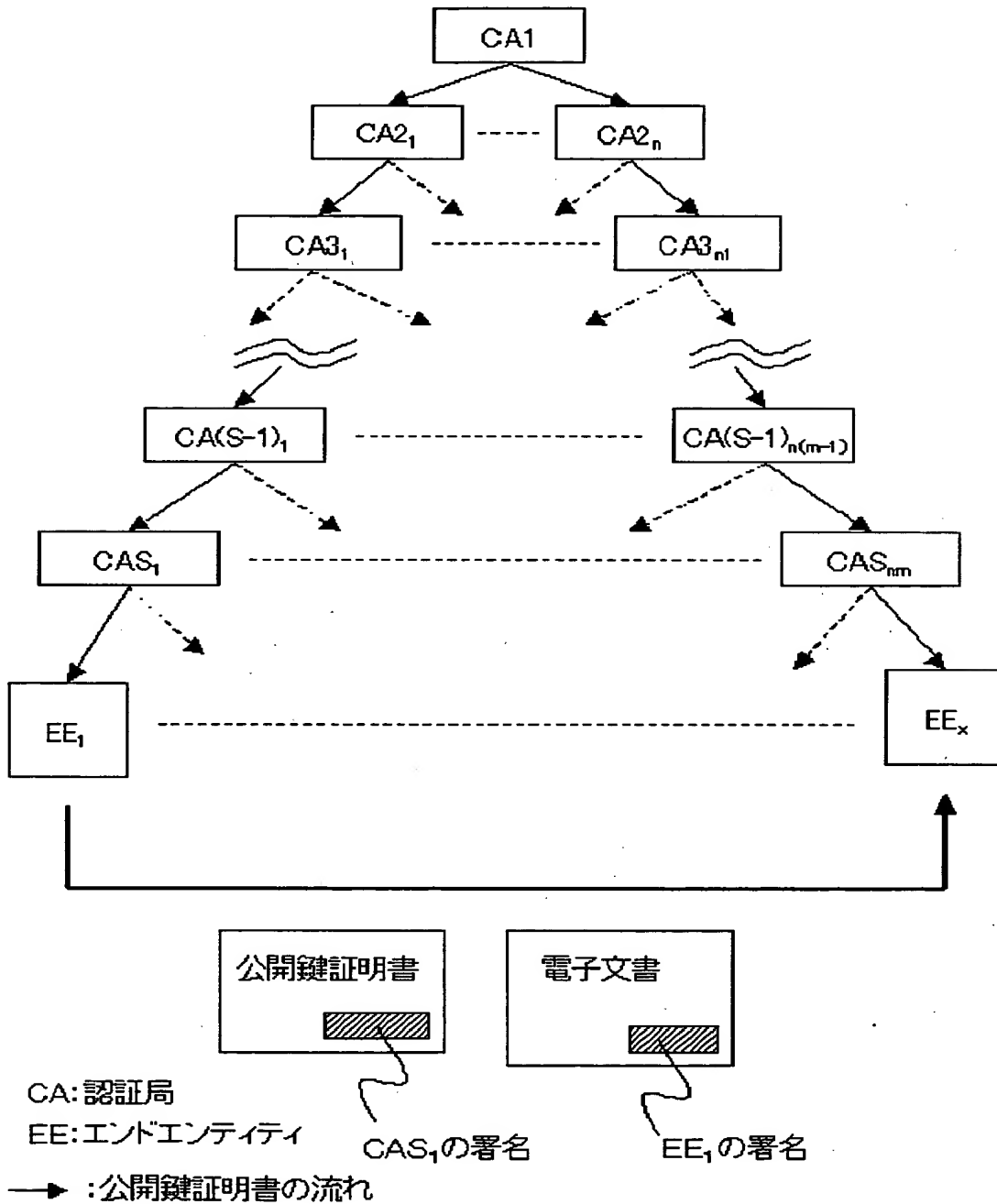
図11

公開鍵証明書の有効性の確認動作



【図 1 2】

図 12



【書類名】 要約書

【要約】

【課題】 公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短縮する。

【解決手段】 証明書有効性確認センタVCは、ブリッジ認証局CA_{bridge}から各端末認証局CAまでのパスの検索、検証を定期的に行い、検証が成立したパスを端末収容認証局に対応付けてパスDBに登録する。また、エンドエンティティEEから証明書の有効性確認依頼があった場合、当該エンドエンティティEEを収容する端末収容認証局CAに対応付けられたパスと依頼対象証明書を発行した端末収容認証局CAに対応付けられたパスとがパスDBに登録されているか否かを調べ、両者が登録されている場合にのみ、当該証明書は有効であると判断する。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所